MATAN SHTEPEL

(925) · 922 · 9254 ◇ matan.shtepel@gmail.com ◇ matanshtepel.com

Last updated: Dec. 2022. ◇ Most recent version: https://matanshtepel.com/matan_shtepel_cv.pdf

OVERVIEW

So far, my research has been in cryptography, with an emphasis on secure multiparty computation (MPC) and oblivious random access memory (ORAM). I am currently in the process of applying to P.h.D programs in (theoretical) computer science.

EDUCATION

University of California, Los Angeles Sep. 2021 - March 2023 (expected)
B.S.E Computer Science with concentration in Pure Math.
GPA: 3.90/4.00 (Ongoing, Fall 2022 factored in)

Research in cryptography
Primary advisor: Prof. Rafail Ostrovsky (UCLA)
Secondary advisor: Prof. Brett Falk (Upenn)

Organized the UCLA Theoretical Computer Science Guild
Organized UCLA Engineering Transfer Center research events

Las Positas Community College June 2020 - May 2021
A.S Computer Science
A.S Math.
GPA: 3.95/4.00

Honors project advised by Dr. William Pezzaglia: Quaternion-based Graphics

PUBLICATIONS

In alphabetical order unless stated otherwise.

- Mark Burgin, Matan Shtepel. On Totalisation of Computable Functions in a Distributive Environment International Journal of Parallel, Emergent and Distributed Systems, Volume 37, Number 3, October 2021.

In-Progress

Out of date. Please see my personal website for an updated list.

- **Asymptotically Efficient Maliciously-Secure DORAM and RAM-MPC**
  We give the first malicious construction of Distributed ORAM while matching the asymptotics of the best-known semi-honest constructions. As a corollary we give the *first* maliciously-secure MPC with logarithmic random access.
  B. Falk, D. Noble, R. Ostrovsky, M. Shtepel, J. Zhang
  Intend to submit to Crypto23 (early February)

- **Practical Maliciously-Secure DORAM & RAM-MPC**
  We construct the most practically efficient DORAM to date. We provide an open-source implementation that we contribute to Xiao Wang's EMP-toolkit. For practical database sizes of upwards of 2^{23} elements, we beat previous constructions (which achieved only semi-honest security) by a factor of at least 100x.
  B. Falk, S. Kelman D. Noble, R. Ostrovsky, M. Shtepel, J. Zhang
  Intend to submit to USENIX23 (early February)

FUNDING & AWARDS

- **NSF REU funding for summer 2022.** Granted for work on secure multiparty computation advised Prof. Rafail Ostrovsky at UCLA.
- **Hack Lodge (sponsored by ETH university) 2023.** Participate in competitively-selected applied cryptography/Ethereum ecosystem focused hacker house.
- **Outliers 23'.** Participate in competitively-selected applied cryptography/web3 focused, VC-backed, summer program.

NON-RESEARCH ACADEMIC ACTIVITIES

Advocate for Community College Researchers Sep 2022 - present
UCLA Engineering Transfer Center

- Create resources to encourage and onboard transfer students into research, including two programs for admitted students in Spring 22.
- Invited to speak on the Engineering Research Presentations & Panel (only transfer student) at UCLA Engineering Day.
- Research-oriented talk Las Positas Community College (expected, January 2023)

Undergraduate Research Mentor Oct 2022 - present
Cryptography research at UCLA

- Induct Stephen Kelman to research, with emphasis on teaching cryptographic implementation. Stephen is now a full coauthor on "Practical Maliciously-Secure DORAM & RAM-MPC."

Founder & Organizer Sep 2022 - present
UCLA TCS Guild

- Start and organize the UCLA Theoretical Computer Science Guild, UCLA's (first?) theoretical computer science community. Meet on a weekly basis, discussing topics in theoretical computer science.

Member Sep 2022 - present
Stanford Decentralized Computing/Blockchain club

- Member of the Stanford Decentralized Computing group ran by Daniel and Priyanka.
- resident of the Summer22' SF hacker-house

Advocate UCLA theoretical CS Modernization present
UCLA CS

- Work with Prof. Sherstov to informally introduce "shiny" modern TCS topics (e.g quantum, (homomorphic) encryption, proof systems) into the UCLA required theory curriculum (CS181).
- hope to generate interest, stir awareness, and show students cool stuff.
- Plan to experimentally introduce those with those topics in Spring23's section of CS181.

WORK EXPERIENCE

Cryptographic advisor Sep 2022 - present
Holonym Foundation (and to a lesser degree, Nexus)

- Advise Holonym Foundation (connecting Web2 to Web3 via ZK) on cryptographic matters, mostly in MPC and ZK, with emphasis on shared-input shared-output psuedorandom functions.
- To a lesser degree, advised Nexus (building blockchain oracles).
- Largely on pause during Fall 2022 due to paper writing and P.h.D. applications, intend to continue in 2023.

STEM Tutor July 2019 - March 2021
Matan's Tutoring Business & Pleasanton Unified School District *Pleasanton, CA*

- Independently tutor middle and high school students primarily in math, but also in biology, programming, and history.
  - Over the entire period, had about 7 students, on average meeting with 3 students a week, each for an hour.
- Tutored for the Pleasanton Unified School District
  - Tutor at Fairlands Elementary School after-school program, twice a week during the 2019 schoolyear until COCIV (march 2019).
  - Tutor at summer school 2019 for english and math.

Founder, Desginer, ... June 2019 - June 2020
RAWGNARLY! (fashion brand) *Pleasanton, CA*

- Founded and operated RAWGNARLY! a fashion brand all about having not-too-serious fun with your friends.
- Sold about 120 garments, both locally in Pleasanton (about 100) and all across the US (about 20).
- Designed garments, photographed lookbooks, created advertisement, built website, negotiated with vendors (US & abroad).

Sales Associate, Pizzaboy August 2018 - May 2019
Skechers & Pizza Guys *Livermore, Pleasanton, CA*

- Retail associate at Skechers Footwear at the Livermore outlets and cook at Pizza Guys' Pleasanton branch.

RELEVANT COURSE WORK

Graduate cryptography sequence + special topics (winter 23'), graduate communication complexity theory, graduate quantum computing, graduate computational complexity theory (winter 23'), graduate theory hits of 21'st century (winter 23'), real analysis sequence, probability theory sequence, linear algebra sequence, group theory, enumerative combinatorics, required CS curriculum.